

IN THE UNITED STATES DISTRICT COURT FOR THE  
DISTRICT OF NEW JERSEY

MALI BU MEDIA, LLC  
Plaintiff,

CASE No. 2:17-cv-12099-KM-JBC

MOTION TO QUASH OR DISMISS  
SUBPOENA

vs.

John Doe, Subscriber IP Address  
173.54.196.218  
Defendants.

\_\_\_\_\_ /

2017 DEC 22 A 9 14  
U.S. DISTRICT COURT  
DISTRICT OF NEW JERSEY  
RECEIVED

**MOTION TO QUASH OR DISMISS SUBPOENA**

**To:** Verizon  
Attn: VSAT  
180 Washington Valley Road  
Bedminster, NJ 07921  
Via Fax: (888) 667-0028  
Customer Service: (800) 837-4966

Defendant John Doe, Subscriber IP Address 173.54.196.218, Docket no. 2:17-cv-12099-KM-JBC moves an order quashing or dismiss the subpoena served upon Verizon as it pertains to John Doe, Subscriber IP Address 173.54.196.218, on the grounds that:

1. It is impossible for Verizon to determine what devices attained the IP addresses when John Doe uses Dynamic Host Configuration Program (DHCP) protocol. The use of dynamically assigned IP addresses means that any device that is connected to a Verizon Cable modem can have different IP addresses based on several different events.

2. Identity of John Doe cannot determine any of the following:
  - a. Whether the device using the Internet connection is a computer, mobile device, tablet, router, etc.
  - b. How many devices may be using a particular IP address to access the internet
  - c. If the MAC address is a true MAC address representing the Ethernet device or one that is spoofed (copied and reused) by some other device (such as a router)
3. In Peer-to-Peer (P2P) file sharing networks, users are typically identified by the IP addresses of their computers. However, most ISPs today assign IP addresses to users dynamically (using the DHCP mechanism). The dynamic reassignment of IP addresses could result in users being falsely accused. *Id.*
4. A specified IP address cannot be assumed to belong to any particular device since the hardware address of a device can be spoofed.
5. It is impossible to say what devices are connected to John Doe's Verizon Internet connection, by whom they were being used, and where the devices were physically located at the time they were being used.
6. In fact, it is impossible for anyone to determine what device negotiated the IP addresses attributed in the Subpoena.
7. Knowing an IP address that was being provided to a cable modem connection does not identify the device is connected through the modem. Even if the copyrighted material in question was being delivered over the Internet through the IP address there is no way to know or prove where it originated or that the owner of the Internet connection with that IP address received the said material.

8. Malibu Media's counsel have been admonished by other courts for similar litigation actions. See *In re BitTorrent Adult Film Copyright Infringement Cases*, 2012 U.S. Dist. LEXIS 61447 at \*28 (E.D.N.Y. 2012) ("in this Case John Does #16 offered the plaintiff "unfettered access" to his computer and employment records demonstrating that he was not at home at the time of the downloading, yet still finds himself pressured to settle for thousands of dollars. It would be difficult to characterize such a resolution as "just" even if speedy.
9. If Malibu Media's copyrights are valid, Malibu has not established a violation by the individual to whom the relevant IP address is registered. As Judge J. Paul Oetken of the Southern District of New York explains,

[t]he fact that a copyrighted work was illegally downloaded from a certain IP address does not necessarily mean that the owner of that IP address was the infringer. Indeed, the true infringer could just as easily be a third party who had access to the internet connection, such as a son or daughter, houseguest, neighbor, or customer of a business offering internet connection.
10. *Patrick Collins, Inc. v. Does 1-6*, No. 12-cv-2964, 2012 WL 2001957, at \*1 (S.D.N.Y. June 1, 2012); see also *In re BitTorrent Adult Film Copyright Infringement Cases*, 296 F.R.D. 80, 84 (E.D.N.Y. 2012) ("[T]he assumption that the person who pays for Internet access at a given location is the same individual who allegedly downloaded a single sexually explicit film is tenuous, and one that has grown more so over time."); *Digital Sin, Inc. v. John Does 1-176*, 279 F.R.D. 239, 242 (S.D.N.Y. 2012) (Judge Nathan

finding that approximately 30% of John Does identified by their internet service providers are not the individuals who actually downloaded the allegedly infringing films). The risk of misidentification is great in a world with ubiquitous Wi-Fi, and given courts' concerns that these sorts of allegations – especially by this plaintiff- are likely to coerce even innocent defendants into settling, the risk of misidentification is important to protect against.” See *Malibu Media, LLC v. John Doe Subscriber assigned IP Address 66108.67.10*, 1:15-cv-04369-AKH (S.D.N.Y. July 2015).


11. For the reasons stated above, it is false and baseless for Malibu Media to say that by knowing the IP addresses of John Doe, Subscriber IP Address 173.54.196.218 that they know who violated their alleged copyright.

WHEREFORE, for the foregoing reasons, Defendant, “John Doe,” respectfully requests that this Honorable Court enter an Order GRANTING this Motion and


1. QUASHING the outstanding subpoena seeking John Doe’s identity;
2. ENTERING a protective order preventing Plaintiff from obtaining further discovery as to Defendant; and
3. FOR SUCH OTHER AND FURTHER RELIEF that this Court deems just and proper.

Respectfully submitted,

Dated: 12/22/2017

*s/John Doe*   
John Doe, Subscriber IP Address  
173.54.196.218  
*Pro se*

CERTIFICATE OF SERVICE

I hereby certify that on 12/22/2017, I served a copy of the foregoing document, via fax  
to: 

**Verizon Legal Compliance**  
**2701 S. Johnson St.**  
**MC: TXD01613**  
**San Angelo, Texas 76904**  
**Fax: 325-949-6916**